

FILED

AUG 10 2017

SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

BRIAN J. STRETCH (CABN 163973)
United States Attorney

BARBARA J. VALLIERE (DCBN 439353)
Chief, Criminal Division

JULIE D. GARCIA (CABN 288624)
Assistant United States Attorney

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
Telephone: (415) 436-6758
FAX: (415) 436-7234
Julie.Garcia@usdoj.gov

Attorneys for United States of America

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

IN THE MATTER OF THE SEARCH OF)	CASE NO. 17-70656
)	
)	UNITED STATES' MOTION TO UNSEAL
)	SEARCH AND SEIZURE WARRANT AND TO
)	REDACT PERSONALLY IDENTIFIABLE
)	INFORMATION THEREIN
)	

Upon the government's application, the Honorable Jacqueline Scott Corley, United States Magistrate Judge for the Northern District of California, granted the government's motion to seal the Application and Affidavit for a Search Warrant, the Search Warrant, and all related papers in the above-referenced matter. *See Exhibit A* (sealing order). Since then, the government has indicted the target of the search warrant. Therefore, the government now moves to unseal all papers in the above-referenced matter.

Because the Application and Affidavit for a Search Warrant and the Search Warrant itself contain personally identifiable information of the defendant and others, the Government further requests that the Clerk be directed to file, in place of the unredacted papers originally filed under seal, the redacted copies attached to this Motion as **Exhibits B, C, and D**. These documents are identical to those

//

1 originally filed under seal except that certain personally identifiable information has been redacted.

2
3 DATED: August 9, 2017

Respectfully Submitted,

4 BRIAN J. STRETCH
5 United States Attorney

6 
7 JULIE D. GARCIA
8 Assistant United States Attorney
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

~~[PROPOSED]~~ ORDER

Based upon the foregoing request, the Court hereby **ORDERS** that:

1. The Application for a Search Warrant, the Affidavit in Support of the Application, the Search Warrant itself, and all related papers in the above-referenced matter shall be unsealed. ✓
2. The Clerk shall file, in place of the unredacted versions originally filed under seal, the redacted copies of the Application for a Search Warrant, the Affidavit in Support of the Application, and the Search Warrant that are attached to the government's Motion as **Exhibits B, C, and D**, which versions redact certain personally identifiable information of the defendant and others.

IT IS SO ORDERED.

DATED: August 9, 2017

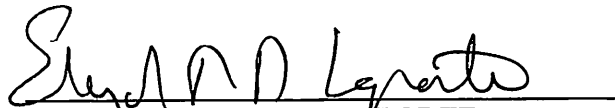

HON. ELIZABETH D. LAPORTE
UNITED STATES MAGISTRATE JUDGE

EXHIBIT A

UNRECORDED

BRIAN J. STRETCH (CABN 163973)
Acting United States Attorney

BARBARA J. VALLIERE (DCBN 439353)
Chief, Criminal Division

JULIE D. GARCIA (CABN 288624)
Assistant United States Attorney

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
Telephone: (415) 436-6758
FAX: (415) 436-7234
julie.garcia@usdoj.gov

Attorneys for United States of America

FILED

MAY 01 2017

SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

JSC

SAN FRANCISCO DIVISION 3-17-70656

IN THE MATTER OF THE SEARCH OF [REDACTED]

[PROPOSED] SEALING ORDER

Good cause appearing therefor, it is hereby ordered that the Motion to Seal, the Application and Affidavit for Search Warrant, the Search Warrant, this Order, and all related papers in the above matter, be filed and maintained under seal until further order of the Court.

DATED: 4/26/17



HONORABLE JACQUELINE SCOTT CORLEY
United States Magistrate Judge

EXHIBIT B

UNITED STATES DISTRICT COURT

for the
Northern District of California

UNDER SEAL
UNDER SEAL

JSC

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Case No. 3-17-70656

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

FILED

MAY 01 2017

SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2252(a)(2)	Receipt or distribution of child pornography
18 U.S.C. § 2252(a)(4)(B)	Possession of child pornography

The application is based on these facts:

See Affidavit of FBI Special Agent Elizabeth Hadley, attached hereto.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Approved as to form:

Julie D. Garcia
AUSA Julie Garcia

Elizabeth Hadley
Applicant's signature

Elizabeth Hadley, FBI Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date:

4/26/17

Jacqueline Scott Corley
Judge's signature

City and state: San Francisco, California

U.S. Magistrate Judge Jacqueline Scott Corley
Printed name and title

EXHIBIT C

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

IN THE MATTER OF THE SEARCH OF

Case No. _____

Filed Under Seal

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Elizabeth J. Hadley, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a warrant authorizing the search of the premises known and described as [REDACTED] (the "SUBJECT PREMISES"), which is located in the Northern District of California. The SUBJECT PREMISES is further described in Attachment A, which is incorporated by reference herein.

2. Based on my training and experience and the facts as set forth in this affidavit, I believe there is probable cause to believe that the SUBJECT PREMISES presently contains contraband, evidence, instrumentalities, or fruits of violations of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B), which prohibit the receipt, distribution and possession of child pornography. I believe there is also probable cause to search the SUBJECT PREMISES, described in Attachment A, for contraband, evidence, instrumentalities, and fruits of these crimes, as further described in Attachment B, which is incorporated by reference herein.

3. Located within the SUBJECT PREMISES to be searched, I seek to seize evidence, fruits, and instrumentalities of the foregoing criminal violations. I request authority to search the entire SUBJECT PREMISES, including the residential dwelling and any computer and computer media located therein, where the items specified in Attachment B may be found. I

also request authority to search the person of Ryan Michael Spencer, date of birth [REDACTED]

[REDACTED] I request authority to seize all items listed in Attachment B as contraband and instrumentalities, fruits, and evidence of a crime.

4. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since 2009. I am currently assigned to the San Francisco Field Office to a squad that investigates crimes against children. Prior to my service with the FBI, I was a Certified Public Accountant. Since joining the FBI, I have investigated, among other things, federal criminal violations related to child pornography and the sexual exploitation of minors. I am currently assigned to investigate cases involving the sexual exploitation of minors, including such exploitation via the Internet and computers. I have experience investigating violations of child pornography and child exploitation and have reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, including computer media. I have participated in the execution of numerous search warrants conducted by the FBI and in the seizure of computer systems and other types of digital evidence.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

APPLICABLE LAW

6. Pursuant to Title 18 U.S.C. § 2252(a)(2), it is unlawful for any person to knowingly receive or distribute any visual depiction of a minor engaging in sexually explicit conduct that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including

by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

7. Pursuant to Title 18 U.S.C. § 2252(a)(4)(B), it is unlawful for any person to knowingly possess or access with intent to view any material that contains any visual depiction of a minor engaging in sexually explicit conduct that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

8. The following definitions apply to this Affidavit and attachments hereto:
- a. “Child Erotica” means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, legally obscene or that do not necessarily depict minors engaged in sexually explicit conduct.
 - b. “Child Pornography” is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

- c. “Computer” is defined in 18 U.S.C. § 1030(e)(1) as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.”
- d. “Computer hardware” consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).
- e. “Computer software” is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- f. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international

borders, even when the devices communicating with each other are in the same state.

g. "Internet Service Providers" ("ISPs") are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line ("DSL") or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider ("ISP") over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

h. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address which is used each time the computer

accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.

i. “Minor” means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

j. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. *See* 18 U.S.C. § 2256(2).

k. “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (“HTML”) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (“HTTP”).

STATEMENT OF PROBABLE CAUSE

9. On April 26, 2017, a federal search warrant for the possession of child pornography was executed on the residence at [REDACTED] Bryan Petersen (“Petersen”), a resident at the [REDACTED] address, was interviewed by Special Agents Elizabeth Hadley and Anastasia Cioni at the scene while the residence was searched.

10. During the course of the interview, Petersen disclosed that he possesses, has distributed and has received images and videos of child pornography. Petersen has received child pornography from several individuals that he met on the Internet. He communicates with these

individuals through Kik messenger¹ and email. Petersen has also met with one of these individuals in person. He identified this person as Ryan Michael Spencer ("Spencer").

11. Spencer is saved in Petersen's phone as Ryan Michael Spencer with the telephone number [REDACTED] and the address [REDACTED]. When shown the Kik messenger application on his phone, Petersen identified the user name "rydawg99" as belonging to Spencer.

12. When shown a California Department of Motor Vehicles photograph for Ryan Michael Spencer, date of birth [REDACTED] Petersen identified the person in the photograph as the person he knows as Ryan Michael Spencer, who uses the Kik account rydawg99.

13. Petersen stated that approximately 12 to 18 months ago he ordered an external hard drive from www.amazon.com and had it delivered directly to Spencer. Spencer and Petersen had agreed that Petersen would send the hard drive to Spencer and that Spencer would put images and videos of child pornography on the hard drive for Petersen. At some point after ordering the hard drive, Petersen traveled to Aptos, California, where Spencer picked him up at a bus station and brought Petersen to his house on [REDACTED]. At that time, Spencer gave a hard drive to Petersen, which Petersen stated contained thousands of images and videos of child pornography.

14. During the execution of the search warrant, the aforementioned external hard drive was seized from Petersen's residence. Petersen identified the bedroom and the external

¹ Kik Messenger is a free instant messenger application for mobile devices from Kik Interactive, available on iOS, Android, and Windows Phone operating systems. Kik Messenger is modeled after BlackBerry Messenger. It uses a smartphone's data plan or Wi-Fi to transmit and receive messages, photos, videos, sketches, mobile webpages, and other content after users register a username.

hard drive as his and provided the password to the hard drive, which was encrypted. The encrypted hard drive was placed into evidence and will be reviewed as soon as possible in a forensic laboratory.

15. Petersen stated that Spencer's primary source of income is from babysitting numerous children and that Spencer takes images and videos of many of these children when they are naked. Spencer told Petersen that his preference is for children approximately four to eight years old. Petersen stated that he has received many images of naked prepubescent children from Spencer via the Kik application.

16. Petersen stated that Spencer claimed to have masturbated one of the children he was babysitting while the child was asleep. Petersen also stated Spencer claimed he had engaged in sexually explicit conduct with several other children while babysitting them.

17. On April 1, 2017, Petersen sent Spencer a message through Kik. He stated "Will send pics tomorrow". The following day, on April 2, 2017 Spencer messaged Petersen on Kik and said "Good... pics??" Petersen then sent one photograph of two prepubescent boys naked in a bathtub, with penis and buttocks visible, and additional photographs of prepubescent boys changing into their pajamas.

18. On April 5, 2017, Spencer sent Petersen numerous images through Kik of prepubescent boys naked in a locker room. In the message following the photos Spencer stated "Boys from [REDACTED] swim lessons".

19. On April 16, 2017, Spencer and Petersen exchanged the following messages:

Petersen	I got something to share
Petersen	[Juvenile Victim #1's] brother like 11 via spycam
Spencer	Share

Spencer He took a spycam vid of his brother? That's hot

Spencer His brother is hot

Petersen I'll probably wait til I get home

Spencer So can't share rn ☹

Spencer Okay

Petersen It's on my laptop now

20. Also on April 16, 2017, referring to the aforementioned video, Spencer sent Petersen Kik messages stating: "Can't wait to see it", "How long? Does he cum", "Gosh I hope [Juvenile Victim #1] gets more", "Ahh so you see his dick and ass thou?"

21. Petersen stated that he has known Juvenile Victim #1 (JV#1) for several years. Petersen stated he recently received from JV#1 via email a video of JV#1's younger brother, Juvenile Victim #2 (JV#2), masturbating in a bathroom. Petersen stated JV#1 told Petersen he had recorded JV#2 without JV#2's knowledge. Petersen stated he saved the video on his laptop. Petersen stated he believes JV#1 is currently 17 years old and JV#2 is approximately ten years old.

22. An FBI Special Agent performed a preliminary review of a laptop seized from Petersen's bedroom during the search of Petersen's residence. During that review, a video file with JV#2's first name in the title was located. The video, which appeared to be surreptitious, depicted a prepubescent male masturbating in a bathroom.

A. Additional information regarding Spencer and the SUBJECT PREMISES

23. On April 26, 2017, I requested a query from the California DMV for Spencer. According to the California DMV database, Spencer's date of birth is [REDACTED] and

his mailing address since at least May 17, 2016 has been [REDACTED]

[REDACTED] the same address listed for Spencer in Petersen's contact list.

24. The residence at [REDACTED] is a tan colored two story residential structure with a brown door on the west side of the residence. Affixed to the right hand side of the door are three white numbers hung vertically "[REDACTED]". The residence has two garages, one attached to the residence and detached on the north-west side of the residence. The two garages are connected by a black steel gate. Both garages have grey doors. In the rear of the property is a brown shed with white trim.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO VIEW AND TRADE CHILD
PORNOGRAPHY**

25. Based upon my knowledge, experience, and training in child pornography and online child exploitation investigations, and on the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in such crimes:

- a. Individuals who distribute, receive, or possess child pornography, and/or seek to engage in the online sexual exploitation of children, or who attempt to commit these crimes, may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, whether in person, in images, or in videos, or in writings describing such activity.
- b. Individuals who distribute, receive, or possess child pornography, and/or seek to engage in the online sexual exploitation of children, or who attempt to commit these crimes, may reinforce their fantasies, often by taking progressive, overt

steps aimed at turning the fantasy into reality in some or all of the following ways: collecting and organizing their child-related material; masturbating while viewing the material; engaging children, online and elsewhere, in conversations, sometimes sexually explicit conversations, to fuel and fortify the fantasy; interacting, both directly and indirectly, with other like-minded adults through membership in organizations catering to their sexual preference for children thereby providing a sense of acceptance and validation within a community; gravitating to employment, activities and/or relationships which provide access or proximity to children; and frequently persisting in the criminal conduct even when they have reason to believe the conduct has come to the attention of law enforcement. These are need-driven behaviors to which the offender is willing to devote considerable time, money, and energy in spite of risks and contrary to self-interest.

- c. Individuals who distribute, receive, or possess child pornography, and/or seek to engage in the online sexual exploitation of children, or who attempt to commit these crimes, may collect sexually explicit or suggestive materials, in a variety of analog or digital media, including photographs, magazines, videos, books, drawings, videotapes, sometimes on reel-to-reel film, or on computer storage devices. These people use these materials for their own sexual gratification, to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to teach a child how to perform various sexual acts.
- d. Individuals who distribute, receive or possess child pornography and/or seek to engage in the online sexual exploitation of children, or who attempt to commit

these crimes, often keep copies of child pornography material; that is, their child pornography collections, correspondence, mailing lists, and related books, whether in digital or other forms, in the privacy and security of their home, or at some other secure location. They prize this material and usually keep it for many years.

- e. Individuals who distribute, receive, or possess child pornography and/or seek to engage in the online sexual exploitation of children, or who attempt to commit these crimes, may correspond with or meet others interested in child pornography so that they can share information and materials. Oftentimes, this correspondence occurs via the Internet and chat-logs, e-mails and records of the correspondence are stored on the users' computers or digital storage media devices. Child pornography collectors often keep lists of names, usernames, e-mail addresses or other contact information for individuals with whom they have been in contact and who share the same interests.
- f. Individuals who distribute, receive or possess child pornography, and/or seek to engage in the online sexual exploitation of children, or who attempt to commit these crimes, commonly create online profiles or user accounts using fake names and images of other individuals or images not attributable to their true selves. These individuals do this in an attempt to conceal their true identities from law enforcement and/or to entice minors for sexual purposes.
- g. Individuals who distribute, receive or possess child pornography, and/or seek to engage in the online sexual exploitation of children, or who attempt to commit these crimes, normally use multiple digital storage media devices, computers and

external storage media in their possession to receive, possess and distribute child pornography and/or other material related to the sexual exploitation of children.

Individuals who use applications on their smart-phones or tablet computers to discuss the sexual exploitation of children or trade child pornography commonly also do so on their personal computers or laptops. Child pornography collectors, and smart-phone and tablet users in general, commonly “sync” their devices with their personal computers or use their personal computers or external storage media to store photos and videos from their smart-phones or tablet computers.

Thus, photos, videos and other files from an individual’s smart-phone or tablet are also commonly found on their personal computers or laptops.

- h. Individuals who distribute, receive or possess child pornography, and/or seek to engage in the online sexual exploitation of children, or who attempt to commit these crimes, prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

26. Based on the facts set forth in the paragraphs above, I believe that Bryan Petersen likely displays characteristics common to individuals who possess, distribute, and/or access with the intent to view child pornography.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

27. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, electronic storage media

devices and the Internet are critical components in the production, distribution, and collection of child pornography.

28. A child pornography image or video taken with a digital camera can be transferred directly to a computer, and then transferred from that computer to any other server or computer connected to the internet via modem or wireless connection. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often have enough space to store thousands of images at high resolution. Video recorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the recorder to a computer. Many devices not traditionally thought of as computers, such as video game consoles, smart-phones, and digital media players, have the ability to store digital data, access the internet, and send or receive digital data electronically.

29. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

30. The large storage capacity of current personal computers, digital storage media devices (e.g. smart-phones or tablet computers), and external hard drives make them ideal repositories for child pornography. External hard drives with capacities of one or more terabytes are inexpensive and common. A terabyte is one thousand gigabytes. An inexpensive and portable flash drive can contain several gigabytes of data. These devices can store thousands of images at very high resolution. Media storage devices can easily be concealed and carried on an individual's person.

31. Child pornography collectors may use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Google and Yahoo!, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

32. Communications made to or from a computer or other digital storage or communications device are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer, or by saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary "cache" folders. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. Such information is often maintained indefinitely until

overwritten by other data. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and the contents of some of the files that were uploaded or downloaded.

33. Computer files or remnants of such files can be recovered years after they were viewed, downloaded, or deleted. Deleted files can often be recovered months or years later using readily available forensic tools. This is because a deleted file does not actually disappear; rather, it remains on the computer's hard drive until it is overwritten by new data. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

34. Based on my experience in conducting and participating in child pornography investigations, images and videos of child pornography are produced and distributed throughout the world, primarily via the Internet. It is common that images and videos of child pornography that offenders possess and distribute include images and videos of known child victims that have been previously identified by law enforcement throughout the United States and the world. This has been corroborated in investigations in which I have conducted and participated based on information provided by the National Center for Missing and Exploited Children in response to submissions of offender's child pornography collections for review to determine which images or videos depict known child victims and where the images were produced. Furthermore, I know

based on my experience and conversations with other law enforcement officers, that computers, computer hard-drives, and other electronic media used to store child pornography are oftentimes manufactured outside of the State of California.

35. I am familiar with the protocol set forth in Attachment C and will abide by the requirements.

//

//

SEARCH METHODOLOGY TO BE EMPLOYED REGARDING ELECTRONIC DATA

36. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. on-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims, and a scan for encryption software;
- b. on-site forensic imaging of any computers that may be partially or fully encrypted, in order to preserve unencrypted electronic data that may, if not immediately imaged on-scene, become encrypted and accordingly unavailable for examination; such imaging may require several hours to complete and require law enforcement agents to secure the search scene until that imaging can be completed;

- c. examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
- d. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- e. surveying various file directories and the individual files they contain;
- f. opening files in order to determine their contents;
- g. scanning storage areas;
- h. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and
- i. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

CONCLUSION

37. Based on the foregoing, I believe there is probable cause to believe that Bryan Petersen has violated the federal criminal statutes cited herein, and that the contraband, evidence, instrumentalities, or fruits of these offenses, more fully described in Attachment B of this affidavit, are located at the SUBJECT PREMISES, described in Attachment A. I respectfully request that this Court issue a search warrant for the SUBJECT PREMISES, including the

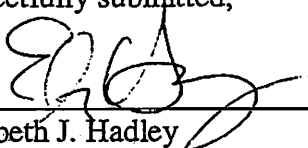
residential dwelling and any computer and computer media located therein, where the items specified in Attachment B may be found. I further request authority to seize the items described in Attachment B.

38. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the return inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

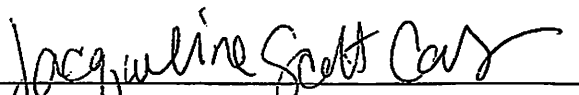
REQUEST FOR SEALING

39. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,


Elizabeth J. Hadley
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me this 26th day of April, 2017



Honorable Jacqueline Scott Corley
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Description of Property to Be Searched

1. The SUBJECT PREMISES at [REDACTED] is a tan colored two story residential structure with a brown door on the west side of the residence. Affixed to the right hand side of the door are three white numbers hung vertically [REDACTED]. The residence has two garages, one attached to the residence and one detached on the north-west side of the residence. The two garages are connected by a black steel gate. Both garages have grey doors. In the rear of the property is a brown shed with white trim.

The premises to be searched includes all rooms, attics, closed containers, and other places therein, any appurtenances to the real property that is the SUBJECT PREMISES of [REDACTED] and any associated storage areas.

This warrant includes the search of the person of Ryan Michael Spencer, date of birth [REDACTED]



ATTACHMENT B

Description of Particular Things to be Seized

The following materials, which constitute contraband, evidence, instrumentalities, or fruits of violations of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B), which prohibit the receipt, distribution and possession of child pornography:

1. Computers or storage media used as a means to:
 - a. visually depict minors engaged in sexually explicit conduct;
 - b. contain information pertaining to a sexual interest in children or in child pornography;
 - c. distribute, receive, or possess child pornography; or
 - d. communicate with or about minors engaged in sexually explicit conduct.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat", instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the COMPUTER user;
- e. evidence indicating the COMPUTER user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. evidence about Internet Protocol addresses used by the COMPUTER;
- l. evidence about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. evidence containing key-word search terms related to child pornography or references to websites related to child pornography; and

- n. contextual information necessary to understand the evidence described in this attachment.
- 3. Routers, modems, and network equipment used to connect computers to the Internet.
- 4. Child pornography and child erotica.
- 5. Records, information, and items relating to violations of the statutes described above including:
 - a. Records, information, and items relating to the occupancy or ownership of [REDACTED] including utility and telephone bills, mail envelopes, or addressed correspondence; Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;
 - b. Records and information relating to the identity or location of the persons suspected of violating the statutes described above; and
 - c. Records and information relating to sexual exploitation of children.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions,

including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

ATTACHMENT C

December 10, 2010, United States District Court for the Northern District of California

PROTOCOL FOR SEARCHING DEVICES OR MEDIA THAT STORE DATA ELECTRONICALLY

THIS PROTOCOL WILL BE ATTACHED TO EACH SEARCH WARRANT THAT AUTHORIZES A SEARCH OF ANY DEVICE OR MEDIA THAT STORES DATA ELECTRONICALLY

1. In executing this warrant, the government will begin by ascertaining whether all or part of a search of a device or media that stores data electronically ("the device") reasonably can be completed at the location listed in the warrant ("the site") within a reasonable time. If the search reasonably can be completed on site, the government will remove the device from the site only if removal is necessary to preserve evidence, or if the item is contraband, a forfeitable instrumentality of the crime, or the fruit of a crime.

2. If the government determines that a search reasonably cannot be completed on site within a reasonable time period, the government must determine whether all or part of the authorized search can be completed by making a mirror image of, or in some other manner duplicating, the contents of the device and then conducting the forensic review of the mirror image or duplication off site. The government will complete a forensic review of that mirror image within 120 days of the execution of the search warrant.

3. In a circumstance where the government determines that a mirror image of the contents of a device cannot be created on site in a reasonable time, the government may seize and retain that device for 60 days in order to make a mirror image of the contents of the device.

4. When the government removes a device from the searched premises it may also remove any equipment or documents ("related equipment or documents") that reasonably appear to be necessary to create a mirror image of the contents of the device or conduct an off-site forensic review of a device.

5. When the government removes a device or related equipment or documents from the site in order to create a mirror image of the device's contents or to conduct an off-site forensic review of the device, the government must file a return with a magistrate judge that identifies with particularity the removed device or related equipment or documents within 14 calendar days of the execution of the search warrant.

6. Within a reasonable period of time, but not to exceed 60 calendar days after completing the forensic review of the device or image, the government must use reasonable efforts to return, delete, or destroy any data outside the scope of the warrant unless the government is otherwise permitted by law to retain such data.

7. The time periods set forth in this protocol may be extended by court order for good cause.

8. In the forensic review of any device or image under this warrant the government must make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, or other electronically-stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

9. For the purposes of this search protocol, the phrase “to preserve evidence” is meant to encompass reasonable measures to ensure the integrity of information responsive to the warrant and the methods used to locate same.

EXHIBIT D

UNDERSEAL

UNITED STATES DISTRICT COURT

for the
Northern District of California**JSC**In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address))
)
) Case No.
)
)
)**3-17-70656****SEARCH AND SEIZURE WARRANT**

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of California
(identify the person or describe the property to be searched and give its location):

See Attachment A.

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

See Attachment B.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or beforeMay 10, 2017
(not to exceed 14 days)☒ in the daytime 6:00 a.m. to 10 p.m.☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge
Hon. Jacqueline Scott Corley

(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) ☐ for _____ days (not to exceed 30).☐ until, the facts justifying, the later specific date of _____.

Date and time issued:

9/26/17 7:50 p.m.
Judge's signatureCity and state: San Francisco, CaliforniaHon. Jacqueline Scott Corley, U.S. Magistrate Judge
Printed name and title

AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of:

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature_____
Printed name and title

ATTACHMENT A

Description of Property to Be Searched

1. The SUBJECT PREMISES at [REDACTED] is a tan colored two story residential structure with a brown door on the west side of the residence. Affixed to the right hand side of the door are three white numbers hung vertically [REDACTED] The residence has two garages, one attached to the residence and one detached on the north-west side of the residence. The two garages are connected by a black steel gate. Both garages have grey doors. In the rear of the property is a brown shed with white trim.

The premises to be searched includes all rooms, attics, closed containers, and other places therein, any appurtenances to the real property that is the SUBJECT PREMISES of [REDACTED] and any associated storage areas.

This warrant includes the search of the person of Ryan Michael Spencer, date of birth [REDACTED]



ATTACHMENT B

Description of Particular Things to be Seized

The following materials, which constitute contraband, evidence, instrumentalities, or fruits of violations of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B), which prohibit the receipt, distribution and possession of child pornography:

1. Computers or storage media used as a means to:
 - a. visually depict minors engaged in sexually explicit conduct;
 - b. contain information pertaining to a sexual interest in children or in child pornography;
 - c. distribute, receive, or possess child pornography; or
 - d. communicate with or about minors engaged in sexually explicit conduct.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat", instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the COMPUTER user;
- e. evidence indicating the COMPUTER user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. evidence about Internet Protocol addresses used by the COMPUTER;
- l. evidence about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. evidence containing key-word search terms related to child pornography or references to websites related to child pornography; and

- n. contextual information necessary to understand the evidence described in this attachment.
- 3. Routers, modems, and network equipment used to connect computers to the Internet.
- 4. Child pornography and child erotica.
- 5. Records, information, and items relating to violations of the statutes described above including:
 - a. Records, information, and items relating to the occupancy or ownership of [REDACTED] [REDACTED] including utility and telephone bills, mail envelopes, or addressed correspondence; Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;
 - b. Records and information relating to the identity or location of the persons suspected of violating the statutes described above; and
 - c. Records and information relating to sexual exploitation of children.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions,

including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

ATTACHMENT C

December 10, 2010, United States District Court for the Northern District of California

PROTOCOL FOR SEARCHING DEVICES OR MEDIA THAT STORE DATA ELECTRONICALLY

THIS PROTOCOL WILL BE ATTACHED TO EACH SEARCH WARRANT THAT
AUTHORIZES A SEARCH OF ANY DEVICE OR MEDIA THAT STORES DATA
ELECTRONICALLY

1. In executing this warrant, the government will begin by ascertaining whether all or part of a search of a device or media that stores data electronically ("the device") reasonably can be completed at the location listed in the warrant ("the site") within a reasonable time. If the search reasonably can be completed on site, the government will remove the device from the site only if removal is necessary to preserve evidence, or if the item is contraband, a forfeitable instrumentality of the crime, or the fruit of a crime.

2. If the government determines that a search reasonably cannot be completed on site within a reasonable time period, the government must determine whether all or part of the authorized search can be completed by making a mirror image of, or in some other manner duplicating, the contents of the device and then conducting the forensic review of the mirror image or duplication off site. The government will complete a forensic review of that mirror image within 120 days of the execution of the search warrant.

3. In a circumstance where the government determines that a mirror image of the contents of a device cannot be created on site in a reasonable time, the government may seize and retain that device for 60 days in order to make a mirror image of the contents of the device.

4. When the government removes a device from the searched premises it may also remove any equipment or documents ("related equipment or documents") that reasonably appear to be necessary to create a mirror image of the contents of the device or conduct an off-site forensic review of a device.

5. When the government removes a device or related equipment or documents from the site in order to create a mirror image of the device's contents or to conduct an off-site forensic review of the device, the government must file a return with a magistrate judge that identifies with particularity the removed device or related equipment or documents within 14 calendar days of the execution of the search warrant.

6. Within a reasonable period of time, but not to exceed 60 calendar days after completing the forensic review of the device or image, the government must use reasonable efforts to return, delete, or destroy any data outside the scope of the warrant unless the government is otherwise permitted by law to retain such data.

7. The time periods set forth in this protocol may be extended by court order for good cause.

8. In the forensic review of any device or image under this warrant the government must make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, or other electronically-stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

9. For the purposes of this search protocol, the phrase "to preserve evidence" is meant to encompass reasonable measures to ensure the integrity of information responsive to the warrant and the methods used to locate same.